



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,621	04/26/2001	Harald Vater	JEK/YATER	8124

23364 7590 11/16/2005

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER

COLIN, CARL G

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 11/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/763,621	Applicant(s) VATER ET AL.	
	Examiner Carl Colin	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 August 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/26/2005 has been entered.

Response to Arguments

2. In response to communications filed on 8/26/2005, Applicant amends claims 1, 3, 9, 11, and 12. Claims 1-18 are presented for examination.

3. In response to communications filed on 8/26/2005, the objection to claims 3 and 11 has been withdrawn in view of the amendment.

3.1 Applicant's arguments, pages 6-7, filed on 8/26/2005, with respect to the rejection of claims 1-18 have been fully considered, but they are not persuasive. Applicant has amended the independent claims to recite that the disguised operation is different than the original operation. However, in a broad interpretation, even disguising the input data x into x' and performing an operation y' on the disguised input data x' is considered as performing a different operation y' , which is different than the original operation y performed on x . Therefore, the claims as

Art Unit: 2136

amended are still anticipated by Kocher. Applicant argues that Kocher does not teach disguising of the DES operation in the manner claimed, but only the input data. Examiner respectfully disagrees. Kocher discloses that the S table lookup operations are also blinded (disguised), they are randomly permuted and reshuffled, therefore, not only the input is disguised with XOR operation, Kocher also suggests disguising the operation (page 2, paragraph 12). On page 5, paragraphs 52-53 and page 6, paragraph 65, Kocher suggests disguising both the input and the operation using reordering, permutation, and randomization. For example, the initial permutation (operation) can be applied to the input message, also the permutation can be applied by manipulating the permutation tables themselves, meaning that the operation is disguised differently than the original before its execution. See also page 4, paragraph 46 and page 7, paragraph 71, and claims 36-37, where both the input and the operations are disguised with the help of XOR as recited in amended claims 3 and 11. As explained above, Applicant has not overcome the rejection by amending the claims, therefore, the claims remain rejected in view of Kocher.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4.1 **Claims 1-18** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Publication US 2001/0053220 to **Kocher et al.**

4.2 **As per claim 1, Kocher et al** discloses a data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that the operation (h) is disguised before its execution, to obtain a disguised operation (h R₁) that is a different operation than the operation (h); for example (see page 2, paragraph 12; page 5, paragraphs 52-54; and page 6, paragraph 65), the disguised operation (h R₁) is executed with disguised input data (x O R₁) , for example (see page 4, paragraphs 46-49; page 7, paragraph 71; and page 6, paragraphs 59-65), and the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h R₁) with disguised input data (x O R₁) yields output data (y) identical with the output data (y) determined upon execution of the operation (h) with undisguised input data (x), whereby disguising operation (h) prevents analysis of said operation (h) and exposure of secret information about said semiconductor chip should a potential attacker

Art Unit: 2136

intercept signal patterns generated during execution of said disguising operation ($h R_1$), for example (see page 4, paragraphs 46-49; page 7, paragraph 71; and page 6, paragraphs 59-65; and page 5, paragraphs 52-54).

As per claim 2, Kocher et al discloses the limitation of a data carrier characterized in that at least one random number (R_1) enters into the determination of the disguised operation ($h R_1$) and the disguised input data ($x \circ R_1$), for example (see page 4, paragraphs 46-49; page 7, paragraph 71; and page 6, paragraphs 59-65).

As per claim 3, Kocher et al discloses the limitation of a data carrier characterized in that the disguised operation ($h R_1$) is generated from the operation (h) with the aid of XOR operations and the disguised input data is generated from the input data (x) with the aid of XOR operations, for example (see page 4, paragraphs 46-49; page 7, paragraph 71).

As per claim 4, Kocher et al discloses the limitation of a data carrier characterized in that the disguised operation ($h R_1$) is permanently stored in the data carrier in advance, for example (see page 2, paragraph 0011).

As per claim 5, Kocher et al discloses the limitation of a data carrier characterized in that at least two disguised operations ($h R_1, h R_1'$) are permanently stored in the data carrier in advance and one of the stored disguised operations ($h R_1, h R_1'$) is selected randomly when a

Art Unit: 2136

disguised operation is to be executed, for example (see page 2, paragraphs 0011-0012 and page 6, paragraphs 59-65).

As per claim 6, Kocher et al discloses the limitation of a data carrier characterized in that the disguised operation (h) R_1 is recalculated before its execution and the at least one random number (R_1) is redetermined for said calculation, for example (see page 7, paragraph 0069).

As per claim 7, Kocher et al discloses the limitation of a data carrier characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y), for example (see page 2, paragraph 0011 and page 10, claim 37).

As per claim 8, Kocher et al discloses the limitation of a data carrier characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1), for example (see page 10, claims 37 and 38).

Claim 9 is similar to claim 1 except for reciting that the disguised operation yields output data which are disguised relative to the output data (y); and the output data can be determined from the disguised output data ($y \oplus R_2$) with the aid of data (R_2) used for disguising the operation (h). **Kocher et al** discloses disguising the output data and the output data can be determined from the disguised output data ($y \oplus R_2$) with the aid of data (R_2) used for disguising

Art Unit: 2136

the operation, for example (see page 4, paragraphs 46-49; page 7, paragraph 71; and page 6, paragraphs 59-65; and page 5, paragraphs 52-54; and page 10, claims 37 and 38).

Claims 10-13 and 15-16 are similar to claims 2-5 and 6-7 respectively except for using a second random number, which is disclosed in the recitations above. **Kocher et al** also discloses using any combination of random numbers (see page 5, paragraph 0051).

As per claim 14, Kocher et al discloses the limitation of a data carrier characterized in that the random numbers (R_1R_2) for determining the first disguised operation ($h R_1R_2$) are inverse to the random numbers ($R_1 \cdot R_2$) for determining the second disguised operation ($h R_1 \cdot R_2$) with respect to the combination used for determining the disguised operations ($h R_1R_2$, $h R_1 \cdot R_2$). **Kocher et al** discloses using two random numbers that can be the same or different, for example (see page 5, paragraphs 0052-54 and page 6, paragraphs 56, 61-65).

As per claim 17, Kocher et al discloses the limitation of a data carrier characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1) and the disguising of the output data (y) contained in the table is effected by combination with the at least one further random number (R_2), for example (see page 10, claims 37 and 38).

As per claim 18, Kocher et al discloses the limitation of a data carrier characterized in that the operation (h) is a nonlinear operation with respect to the combination used for disguising the operation (h), for example (see page 2, paragraph 0011 and page 10, claim 37).

Conclusion


5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
November 10, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100